(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－518651
（P2001－518651A）
(43)公表日　平成13年10月16日(2001.10.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ	5/00	５Ｃ０５９
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ	1/387	５Ｃ０７５
1/44			1/44	５Ｃ０７６
7/24			7/13	Ｚ　５Ｊ１０４

審査請求　未請求　予備審査請求　有　（全 47 頁）

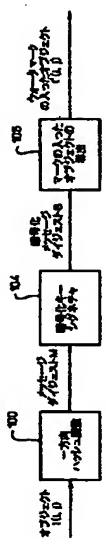
(21)出願番号　特願2000－514463(P2000－514463)
(86)(22)出願日　平成10年９月24日(1998.9.24)
(85)翻訳文提出日　平成12年３月27日(2000.3.27)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／２０１９６
(87)国際公開番号　ＷＯ９９／１７５３７
(87)国際公開日　平成11年４月８日(1999.4.8)
(31)優先権主張番号　０８／９３９，２１５
(32)優先日　平成９年９月29日(1997.9.29)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ヒューレット・パッカード・カンパニー
ＨＥＷＬＥＴＴ－ＰＡＣＫＡＲＤ　ＣＯＭＰＡＮＹ
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　ナタラヤン，パラス，ケイ
アメリカ合衆国カリフォルニア州95030，ロスゲイトス，リード・クノル・ロード・18079
(74)代理人　弁理士　古谷　馨　（外２名）

最終頁に続く

(54)【発明の名称】　デジタルオブジェクトのウォータマーキング

(57)【要約】
デジタルウォータマークを利用して、デジタルオブジェクトを識別するための技法である。この技法には、デジタルオブジェクトのソースデータから導き出されたメッセージを暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るステップと；暗号化メッセージダイジェスト（Ｓ）からウォーターマークを導き出すステップと；ソースデータにこのウォーターマークを組み込むステップを含む。暗号化は、公開キー暗号化システムによって実施されることが好ましい。暗号化されるメッセージは、デジタルオブジェクトのソースデータに対しハッシュ関数で処理を施すことによって得ることができ、メッセージダイジェスト（Ｍ）が得られる。このメッセージデジタル（Ｍ）は、シグネチャ暗号化キーによって暗号化されたメッセージであり、暗号化メッセージダイジェスト（Ｓ）が得られる。ウォーターマークは、クロッピング、スケーリング、切り捨てに対して耐性がある。



【特許請求の範囲】

【請求項１】デジタルウォータマークを利用して、デジタルオブジェクトを識別するための方法であって、

（ａ）前記デジタルオブジェクトのソースデータから導き出されるメッセージを暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るステップと、

（ｂ）前記暗号化メッセージダイジェスト（Ｓ）からウォータマークを導き出して、前記ソースデータに組み込むステップと

を含む方法。

【請求項２】前記メッセージが、前記デジタルオブジェクトの前記ソースデータにハッシュ関数を実行して、前記デジタルオブジェクトのメッセージダイジェスト（Ｍ）を得ることによって得られることと、前記メッセージダイジェスト（Ｍ）が、前記暗号化メッセージダイジェスト（Ｓ）を得るために、シグネチャ暗号化キーによって暗号化されたメッセージである、請求項１に記載の方法。

【請求項３】前記ウォータマークが物理領域のウォータマークであり、さらに前記ソースデータの少なくとも一部に前記物理領域のウォータマークを組み込むステップが含まれる、請求項１に記載の方法。

【請求項４】さらに前記ウォータマークを導き出す際、前記暗号化メッセージダイジェスト（Ｓ）から導き出された周波数領域ベクトル（Ｕ）を物理領域に変換するステップを含む、請求項３に記載の方法。

【請求項５】さらに前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調して、前記周波数領域ベクトル（Ｕ）の少なくとも一部を得ることによって、前記周波数領域ベクトル（Ｕ）を導き出すステップを含む、請求項４に記載の方法。

【請求項６】前記周波数領域ベクトル（Ｕ）の一部が低周波数に対応し、前記周波数領域ベクトル（Ｕ）の別の一部が高周波数に対応し、低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調することによって導き出される、請求項５に記載の方法。

【請求項７】低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、

前記ウォータマークの振幅に対して、高周波数に対応する前記周波数領域ベクトル（Ｕ）の一部よりも重要な影響を及ぼすように変調されている、請求項６に記載の方法。

【請求項８】低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部の「０」ビットに対応する要素に負の値を有し、かつ前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部の「１」ビットに対応する要素に正の値を有し、高周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、ゼロ値の要素を備える、請求項７に記載の方法。

【請求項９】前記ソースデータがピクセルの行及び列から構成され、前記ウォータマークが、前記ピクセルの前記行の数（ｍ）又は前記列の数（ｎ）に対応する次元を備えるウォータマークベクトル（Ｗ）によって表される、請求項１に記載の方法。

【請求項１０】ピクセルが、イメージオブジェクトの離散的セクションに関するデータを含む、請求項９に記載の方法。

【請求項１１】ピクセルが、オーディオオブジェクトの離散的セクションに関するデータを含む、請求項９に記載の方法。

【請求項１２】前記ソースデータに組み込まれる前記ウォータマークが、前記ウォータマークを付加されるデータに対して直交する、請求項９に記載の方法。

【請求項１３】さらに前記ソースデータの少なくとも一部を選択することによって、前記ソースデータからウォータマークベクトル（Ｗ）と同じ次元を備えたソースデータベクトル（Ａ）を導き出すステップを含み、さらに前記ウォータマークベクトル（Ｗ）がソースデータベクトル（Ａ）と直交するように、前記暗号化メッセージダイジェスト（Ｓ）に基づいて前記ウォータマークベクトル（Ｗ）を導き出すステップを含み、さらに前記ウォータマークベクトル（Ｗ）と、ソースデータベクトル（Ａ）が導き出される前記ソースデータの前記選択部分におけるデータを組み合わせて、ウォータマークの入ったデータを形成するステップを含む、請求項９に記載の方法。

【請求項１４】さらに前記ウォータマークの組み込み前を前記ウォータマークの組み込み後に対して、前記ソースデータの少なくとも一部を比較するステップを含む、請求項９に記載の方法。

【請求項１５】さらに前記ウォータマークベクトル（Ｗ）と前記ウォータマークを含んでいることが疑われるデータから導き出される目標ベクトル（Ｘ）との間の相関関係を見出すステップを含み、前記目標ベクトル（Ｘ）が、前記ウォータマークの組み込まれている前記ソースデータに対して直交する、請求項１４に記載の方法。

【請求項１６】デジタルウォータマークを利用してデータを識別するための方法であって、

（ａ）ソースデータに一方向関数を実行して、メッセージダイジェスト（Ｍ）を得るステップと、

（ｂ）シグネチャ暗号化キーによって前記メッセージダイジェスト（Ｍ）を暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るステップと、

（ｃ）前記暗号化メッセージダイジェスト（Ｓ）の高周波数に対応する部分より多い低周波数に対応する部分を変調することによって、前記暗号化メッセージダイジェスト（Ｓ）から周波数領域ベクトル（Ｕ）を導き出すステップと、

（ｄ）前記周波数領域ベクトル（Ｕ）を物理領域キーベクトル（Ｖ）に変換するステップと、

（ｅ）前記ソースデータの一部を選択して、前記選択されたソースデータに直交する周波数領域ベクトル（Ｕ）からウォータマークベクトル（Ｗ）を導き出すステップと、

（ｆ）前記選択されたソースデータと前記ウォータマークベクトル（Ｗ）を物理領域において組み合わせるステップと

からなる方法。

【請求項１７】デジタルウォータマークを利用してデータを識別するためのシステムであって、

（ａ）シグネチャ暗号化キーによってソースデータから導き出されるメッセージを暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るための手段と、

（ｂ）前記暗号化メッセージダイジェストからウォータマークを導き出して、前記ソースデータに組み込むための手段と
を含むシステム。

【請求項１８】さらに前記ソースデータにハッシュ関数を実行して、メッセージダイジェスト（Ｍ）を得るための手段を含み、前記暗号化するための手段が、前記シグネチャ暗号化キーによって前記メッセージダイジェスト（Ｍ）を暗号化して、前記暗号化メッセージダイジェスト（Ｓ）を得る、請求項１７に記載のシステム。

【請求項１９】前記ウォータマークが物理領域ウォータマークであり、前記導き出す手段が、前記物理領域ウォータマークを前記ソースデータの少なくとも一部に組み込む、請求項１７に記載のシステム。

【請求項２０】前記導き出す手段が、前記暗号化メッセージダイジェスト（Ｓ）から周波数領域ベクトル（Ｕ）を導き出し、前記ウォータマークを導き出す際、前記周波数領域ベクトル（Ｕ）を物理領域に変換する、請求項１９に記載のシステム。

【請求項２１】前記導き出す手段が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調し、前記周波数領域ベクトル（Ｕ）の少なくとも一部を得ることによって、前記周波数領域ベクトル（Ｕ）を導き出す、請求項２０に記載のシステム。

【請求項２２】前記導き出す手段が、前記ソースデータをピクセル行及び列として管理し、前記周波数領域ベクトル（Ｕ）に基づいてウォータマークベクトル（Ｗ）を導き出し、前記ウォータマークベクトル（Ｗ）が、前記ピクセルの行の数（ｍ）又は前記列の数（ｎ）に対応する次元を備えている、請求項２１に記載のシステム。

【請求項２３】前記導き出す手段が、前記ソースデータの少なくとも一部を選択することによって、前記ソースデータから前記ウォータマークベクトル（Ｗ）と同じ次元を備えるソースデータベクトル（Ａ）を導き出し、前記ウォータマークベクトル（Ｗ）が、ソースデータベクトル（Ａ）に直交する、請求項２２に記載のシステム。

【請求項２４】さらに目標データセットを前記ソースデータと比較するための手段が含まれ、前記比較するための手段が、前記目標データから導き出された目標ベクトル（Ｘ）を前記ソースデータと比較し、前記目標ベクトル（Ｘ）が前記ソースデータベクトル（Ａ）に対して直交する、請求項２３に記載のシステム。

【請求項２５】コンピュータによる読み取りが可能なプログラムコード手段を具体的に体現し、デジタルウォータマークを利用して、コンピュータにデジタルオブジェクトを識別させる、プログラム記憶媒体を備える製品であって、

（ａ）前記デジタルオブジェクトのソースデータに対して一方向関数を実行して、前記ソースデータのメッセージダイジェスト（Ｍ）を得るためのコード手段と、

（ｂ）シグネチャ暗号化キーによってメッセージダイジェスト（Ｍ）を暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るためのコード手段と、

（ｃ）周波数領域としての前記メッセージダイジェスト（Ｓ）の一部を物理領域に変換することによって、前記暗号化メッセージダイジェスト（Ｓ）からウォータマークを導き出した後、前記ソースデータに組み込む一次元ウォータマークが得られるようにするためのコード手段と、

（ｄ）前記一次元ウォータマークを前記ソースデータに組み込むためのコード手段と

が含まれている製品。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルデータにウォータマーキング（電子すかし入れ）を施すための技法に関し、より詳細にはイメージ及びオーディオデータのようなデジタルデータに著作権所有を認証するために施すウォータマーク（電子すかし）に関する。

【０００２】

【従来の技術】

近年電子商取引が急速に増大しているため、保全データのトランザクションがますます重要になっている。電子データが無許可者によって盗用されるのを阻止するため、他者への意図せぬ露見から保護するため、賛同者間におけるデジタルデータの伝送は、暗号方式を利用して行われている。データ保護のため、暗号手法によって、軍事情報、金融取引、個人データ等を含む各種データを伝送することが可能である。

【０００３】

従来、オリジナル技術又は著作物に対する権利を保護する領域において、大部分の侵害は、無許可者が、オリジナル（例えば著作権のある）作品の許可されたコピーの物理的コピーを作成することによって行われた。著作権のある絵画、写真、レコード及びアナログオーディオテープといった物理的芸術資料のコピーは、通常オリジナルよりも知覚上劣っている。例えば写真複写又は写真によるコピープロセスにおける忠実度の劣化は、こうした資料の無許可のコピーを思いとどまらせる要因の１つである。今日では、多くのビジュアル、オーディオ、書籍又は他の著作権を有する作品は、デジタル方式で記憶され、伝送される。こうしたデジタル資料は、あまり忠実度を損なうことなく、繰り返しコピーすることが可能である。オリジナルの芸術作品、すなわち著作権のある作品の所有権者にとってのリスクは、デジタルデータがいったん伝送されると、その伝送データのコピーの疑いのあるデータを見つけた場合、その疑いのあるデータが、元の伝送データ、例えば１つの芸術作品のデジタルデータからコピーされたものであるか否か

の検証が、通常不可能であるという点である。

【０００４】

最近、例えば著作権を守らせるため、デジタル資料源の識別を容易にするデジタルウォータマーキングが、機密保護技法として考案された。ウォータマークは、オリジナルデジタルデータに埋め込まれた識別コードであり、芸術作品を観察する人間には気付かれないことが望ましい。あるウォータマーキング方式の例では、デジタルオーディオ信号に識別ストリングを挿入し、ランダムに選択されたオーディオサンプルの重要ではないビットを識別コードのビットに置換することを必要とする。ビデオデジタル作品に対するウォータマーキングに関連した別のウォータマーキングの例では、修正する場合、ビデオ信号を正確に復合化するには、複数の他のパラメータを修正しなければならない、所定の符号化パラメータに対して所定の値を割り当てることが必要とされる。あるウォータマーキング技法では、オブジェクトの各コピーに、識別コードにマーキングが施される。さらに最近になって、イメージに２次元スペクトラム拡散信号が付加されるウォータマーキング方式が提案されている。所定のイメージにおけるウォータマークを確認するため、所定のイメージからオリジナルイメージを減算し、差分イメージとウォータマーク信号の相関関係が計算される。

【０００５】

デジタルデータに対するウォータマーキングは大幅に進歩したが、一般に先行するウォータマーキング技法には、種々の欠点がある。多くの場合、ウォータマークの存在を確認するために、オリジナルイメージが必要になる。作品の一部を削除するクロッピング、及び作品のサイズを拡大又は縮小するためのスケーリングといった処理操作によって、確認プロセスにかなりの問題が生じる。多くの場合、ウォータマーキング方式は可逆性である、すなわちアタッカー（又は改竄者）は、最初のウォータマークの入ったイメージに基づいて、ただし最初のウォータマークがいかなるものであるかについての知識がなくても、第２のイメージ及び第２のウォータマークを計算し、第２のウォータマークを第２のイメージに挿入することによって、結果として最初のウォータマークの入ったイメージを得ることができる。こうした可逆性ウォータマーキング方式によって、著作権を有す

る作品の認証されたコピーの確認が困難になる可能性がある。さらに不徳者が他人のウォータマークの入った資料を盗用し、その資料から自分のウォータマークを減算し、結果生じる作品を自分のものであると主張する可能性があるので、貴重なデジタルデータに関する所有権紛争を生じることさえある。先行するウォータマーキング技法では、コントラスト又は輝度の変化によって、確認アルゴリズムがだまされる場合が多く、その信頼性を低下させている。さらにウォータマーキング方式の多くは、ウォータマークを生成し、管理するための手法が得られない。これは、同じウォータマークを用いていくつかの作品が保護される場合、ウォータマークの機密が漏洩すると、全ての作品の保護が危険にさらされることを意味している。これらの欠陥を克服することが可能なウォータマーキング技法が必要とされている。

【０００６】

【発明が解決しようとする課題】

したがって本発明の目的は、クロッピングに耐え、可逆性であり、輝度又はコントラストの変化に耐える、また１つのウォータマークの入った作品におけるウォータマーキング技法が開示されても、他の関連するウォータマークの入った作品を危険にさらすことのない、ウォータマーキング技法を提供することにある。

【０００７】

【課題を解決するための手段】

本発明によれば、デジタルウォータマークを利用してデジタルオブジェクトを識別するための技法が提供される。この技法は、コンピュータを利用して容易に実施することが可能である。この技法には、デジタルオブジェクトにおける一組のソースデータから導き出されるデータを暗号化することと、暗号化データからウォータマークを導き出すことと、ウォータマークをソースデータに組み込むことが含まれる。ハッシュ関数によってデジタルオブジェクトのソースデータが処理されて、デジタルオブジェクトのメッセージダイジェスト（Ｍ）が求められ、シグネチャ暗号化キーによって、メッセージダイジェスト（Ｍ）が暗号化されて、暗号化メッセージダイジェスト（Ｓ）が求められるようにするのが望ましい。さらにメッセージダイジェスト（Ｍ）の暗号化は、公開キー－私用キー暗号化シ

ステムによって実施されることが望ましい。望ましい態様は、一方向ハッシュ関数によってソースデータに処理を施して、メッセージダイジェストを得ることであるため、明瞭かつ便利なように、ソースデータの組から導き出される暗号化のためのデータセットは、本明細書において「メッセージ」又は「メッセージダイジェスト」と呼ばれるが、必ずしも一方向ハッシュ関数による処理を受けたものである必要はない。暗号化データの組は、同じ理由から、本明細書において「暗号化メッセージダイジェスト」と呼ばれる。

【０００８】

本発明のウォータマーキング技法は、汎用性があり、オーディオ、ビデオ、イメージ、マルチメディアデータ等を含む種々のデジタルオブジェクトにウォータマークを入れるのに有効に使用することが可能である。さらに本技法は、アタッカーが容易に攻撃できないので、高度な機密保護が得られる。例えば本技法では、私用キーが秘密を保持される暗号化に関連したハッシュ関数を利用することによって、多くの先行するウォータマーキング技法とは異なり、可逆性ではないという利点が得られる。したがってアタッカーが、即値情報の開示によってオリジナルのウォータマークを逆算することは極めて困難である。さらに機密を高めるために、本発明の一実施態様では、公開キー暗号化システムが利用される。結果として、オリジナルオブジェクトの所有権者の公開キーによって、疑わしいオブジェクト（すなわち、オリジナルの、例えば著作権のあるオブジェクトからコピーされた疑いのあるオブジェクト）をチェックし、他のウォータマークの入ったオブジェクトを危険にさらすことなく、そのウォータマークが存在するか否かを判定することが可能になる。公開キーを必要とする暗号化技法が用いられる実施態様の場合、オブジェクトの所有権は、所有権者がその私用キーを明らかにすることを必要とせずに、オブジェクトの所有権者の公開キーだけを利用して、法廷のような中立者に対して確認させることが可能である。またウォータマークが、損失のある圧縮（データファイルのサイズを縮小するため、知覚上重要性の劣る情報が省かれる）又はクロッピング（オブジェクトの一部が削除される）によって取り除かれることはない。ウォータマークベクトルが、ウォータマークを挿入することになるピクセルのベクトルに対して直交する実施態様の場合、輝度又は

コントラストの変化によって、確認アルゴリズムがだまされることはない。

【０００９】

【発明の実施の形態】

以下の図面は、よりよく図解された本発明の技法の実施態様を含む。これらの図面では、いくつかの図面において同様の参照番号が同様の造作を示す。

【００１０】

本発明によれば、デジタルオブジェクトにデジタルウォータマークを挿入し、ウォータマークについてデジタルオブジェクトの評価を行うための技法が提供される。ウォータマークの導出には、暗号化技法が用いられ、ウォータマークは、アタッカー（すなわちウォータマークの入ったデータを改竄して、ウォータマークを除去又は変更する者）が、ウォータマークの入ったデジタルオブジェクトからオリジナルデジタルオブジェクトを導き出すのを極めて困難にするようなやり方で、デジタルオブジェクトに組み込まれる。このデジタルウォータマークには、クロッピング、スケーリング、不注意による歪み、並びにアタッカーによるウォータマークの故意による除去又は破損に対する耐性がある。

【００１１】

本発明の技法によってウォータマーキングを施すことができるデジタルオブジェクトは、デジタルビジュアルイメージ；例えば音楽のようなデジタルオーディオプログラム；例えば接触によって感知することができる触覚情報に変換可能なデータのような、デジタル触覚データ；マルチメディアデータ；又は「ピクセル」の行及び列に構成し得る個別セグメントに分割することが可能な単なるデジタルデータストリングとすることができるので、「物理的オブジェクト」と呼ばれる。イメージの場合、こうしたピクセルの明瞭な一例が、カラー写真を走査して、カラードット（一般に視覚表示テクノロジにおいて「ピクセル」として知られる）の行及び列を表したデジタル情報にすることによって得られる、デジタル情報のピクセルということになろう。したがってデジタル化写真には、数百のピクセル行及び列が含まれる。しかし本開示において、「ピクセル」は、例えば上述のような、他のタイプのデジタル情報に関するデジタルデータの個別セグメントとすることが可能である。例えば録音の場合、Ａ／Ｄ変換器によって音声信号の

サンプリングを行い、特定の時間セグメントにおける音声信号の特性を表す値を備えたサンプルを出力することが可能である。ビジュアルイメージ、オーディオ信号及び他のデータストリームに関するデータのピクセルを得るための技法は、当該技術において周知である。デジタルオブジェクトを得るための任意の従来の技法を適用することが可能である。もう１つの例として、デジタルカメラ又はコンピュータグラフィックスソフトウェアを実行するコンピュータを使用して、デジタルイメージを直接発生することが可能である。同様に、音楽は、Ａ／Ｄ変換器を利用して、音波からデジタルデータに変換することができる。これらのデジタルオブジェクト及び他のタイプのデジタルオブジェクトは、本発明に適用可能である。

【００１２】

図１には、本発明のウォータマーキング技法の実施態様の１つが描かれている。ハッシュ関数100（例えばMD5関数のような一方向ハッシュ関数）によって、ｍ行及びｎ列のピクセルを備えるデジタルオブジェクト、ベクトル$I_V(i,j)$に処理を施し、結果としてメッセージダイジェスト、ベクトルM_Vが得られる。ハッシュ関数の機能は、入力データ$I_V(i,j)$受け取って、固定サイズストリング（ハッシュ）、好ましくはほぼ指紋（fingerprint）ほどの、入力データ$I_V(i,j)$の大きいオブジェクトに関して、はるかに短いストリングに変換することである。ハッシュは、ハッシュすなわちメッセージダイジェストM_Vからオリジナル入力データを生成するのが極めて困難になるように生成されるのが望ましい。この逆算の困難さは、アタッカーがハッシュから入力データを導き出すことが可能な場合、ウォータマークを除去又は変更する可能性があるので有益である。当該技術において、多くのハッシュ関数が既知であり、本技法に適用可能である。当該技術において既知の、適用可能な一方向ハッシュ関数（又はメッセージダイジェストアルゴリズム）の１つに、MD5法がある。他の適用可能な一方向ハッシュ関数の例には、SNEFRU関数、SHA関数及びHAVAL関数がある。（一方向ハッシュ関数に関する解説については、Schneier,B.,Applied Cryptography,Jhon Wiley and Sons,1993,pp.333-346を参照されたい。）当該技術者には、こうしたハッシュ関数をデジタルオブジェクトに適用する方法が明らかであろう。一般に、固定長

のハッシュ値ｈを取得するため、任意の長さのメッセージ、ベクトルF_Vに操作を加えるハッシュ関数Ｈ（F_V）を選択する場合、ｈは

ｈ＝Ｈ（M_V）、

であり、次の特性が所望される：Ｍが与えられたとすると、ｈの計算が容易である；ｈが与えられたとすると、Ｍの計算が困難である；Ｍが与えられたとすると、Ｈ（Ｍ）＝Ｈ（Ｍ’）の特性を満足する、他のメッセージＭ’を見つけるのが困難である。ハッシュ関数は、バースデイアタック（Birthday attack）だけでなく、同じハッシュ関数によって同じ値を戻す２つのランダムメッセージの発生に基づく、やみくもな強制的アタックにも耐えるように選択するのが望ましい。

【００１３】

次にメッセージダイジェストM_Vがシグネチャによって暗号化される。暗号化アルゴリズムは、公開キー－私用キーシステム（非対称データ暗号化アルゴリズム）又は私用キーシステム（対称データ暗号化アルゴリズム）とすることが可能である。こうした暗号化によって、これらの暗号化データと他のデータを識別し、したがって物理的文書の物理的シグネチャとほぼ同じ働きをする独自の機能がメッセージダイジェスト、ベクトルM_Vに付与される。私用キーだけを用いて暗号化する場合、この私用キーによって、オリジナルメッセージの機密が保護されていて、暗号化メッセージダイジェストは可逆性である、すなわちアタッカーは、暗号化メッセージダイジェストから、メッセージダイジェストM_V又はオリジナルオブジェクトを逆算することができない。しかし例えば法廷のような第三者に対して所有権を立証する必要があれば、所有権者のシグネチャを確認するため、所有権者はその私用キーを明かさなければならないであろう。私用キーが明らかになると、アタッカーは、その私用キーに対するアクセスを獲得して、他のオブジェクトのウォータマークに関する情報を取得することができる可能性があるので、同じか又は同様の私用キーウォータマークによってマーキングされた所有権者の他のウォータマークが入ったオブジェクトが危険にさらされる可能性がある。

【００１４】

より望ましい方法は、公開キー－私用キー暗号化システム（別段の指定がない

限り、今後は「公開キーシステム」と称する）を利用することである。公開キーシステムを利用した暗号化の場合、ユーザは、整合する１対のキー、すなわち私用キーと公開キーを所持する。私用キーは、秘密にしておかれ、ユーザだけしか知らないが、公開キーは、広く提供することが可能である。いずれかのキーで暗号化されたメッセージは、もう一方のキーでしか解読することができない。ユーザが私用キーでメッセージを暗号化すると、そのメッセージはユーザの公開キーでしか解読することができない。ユーザだけしかその私用キーを所有していないので、暗号化メッセージは、ユーザの公開キーでしか解読することができない。私用キーは暗号化した者にしか分からないので、暗号化メッセージがユーザの公開キーで解読可能である場合、ユーザが、その「シグネチャ」を用いて、メッセージを暗号化しなければならなかった、すなわちユーザが、そのメッセージに「サイン」したということが立証される。シグネチャの強度は、ユーザの公開キーが本物であることを知っているかどうかによって決まる。このため、公開キーは第三者によって公証又は認証されるのが望ましい。本発明では、公開キーシステムが利用される場合、私用キーを利用してメッセージの暗号化を行い、オリジナルイメージからウォータマークが生成される。ウォータマークの所有権を立証する必要がある場合、所有権者のシグネチャを確認するため、例えば確認を行う第三者に公開キーを与えることが可能である。本発明における公開キー暗号化を利用する利点は、私用キーを使用してオリジナルオブジェクトからウォータマークを生成するので、アタッカーが、公開キーにアクセスしたとしても、私用キーなしでは、ウォータマークの入ったオブジェクトからウォータマークを除去して、偽オリジナルを生成するのが不可能か、又は極めて困難になるという点にある。

【００１５】

私用キーシステムと公開キーシステムのいずれの場合にも、暗号化されたM_Vから逆算して、オリジナルのM_Vを得るためには、暗号化アルゴリズムの私用キーが必要になる。当該技術において、多くの暗号化アルゴリズムが既知であり、この目的に利用することが可能である。良い例がRSAアルゴリズムである。他の適用可能な公開キーアルゴリズムには、ELGAMALアルゴリズム及びDSS（デジタルシグネチャ規格）アルゴリズムが含まれる。例えばPOHLIG-HELLMANアルゴリズム

、RABINアルゴリズム及びDES（デジタル暗号化規格）アルゴリズムといった、他の多くの暗号化アルゴリズムも既知であり、上述のSchneier,B.,Applied Cryptographyを参照されたい。当該技術者には、こうした暗号化アルゴリズムをデジタルオブジェクトに適用する方法が分かるであろう。

【００１６】

私用キーが秘密にされている限りにおいて、公開キーシステムと私用キーシステムのどちらか任意のシステムを利用した暗号化ステップを用いて、ハッシュ関数による処理を伴わずに、デジタルオブジェクトを直接暗号化することができるという点に留意されたい。しかしデジタルイメージが大きい場合、極めて長い計算時間が必要になる。ハッシュ関数によれば、ウォータマークの生成に暗号化を必要とするデータサイズが縮小される。

【００１７】

暗号化メッセージダイジェスト、ベクトルS_Vが形成された後、それに処理を施して（ブロック106）ウォータマークの入ったオブジェクト、ベクトルI_V'（i,j）が導き出される。図２に示す実施態様の場合、ウォータマークの入ったオブジェクトI_V'（i,j）を導き出すために、暗号化メッセージダイジェストS_Vは変調され、例えばその信号の振幅に変調を施して、そのスペクトルの知覚上重要な領域にわたる拡散が行われる（ブロック108）。このプロセス（ブロック108）によって、物理領域信号を表すキーベクトルV_Vが得られる。スペクトルの大部分にわたってメッセージダイジェスト、ベクトルS_Vを拡散させることには、ウォータマークをオブジェクトの設計対象となる人間の感覚器官ではほとんど知覚できないようにするという利点がある。さらにデータが圧縮又はクロッピングといったプロセスによって操作を加えられる場合に、ウォータマークは保存されることになる。例えばスペクトルのかなりの部分にわたってメッセージダイジェストS_Vを拡散すると、ビジュアルイメージのある一定の狭い範囲のカラー、あるいはある一定の狭い範囲のオーディオ周波数が過度に歪むことがなくなる。有用なウォータマークは、損失のある圧縮又はクロッピングを受ける際、保護されるのが望ましいので、スペクトル部分の知覚上重要なスペクトル周波数部分に配置される。（例えばアタッカーが）こうしたウォータマークの入ったオブジェクトに

クロッピングを施して、ウォータマークを除去すると、オブジェクトは十分に歪むので、その品質は、オリジナルのオブジェクト又はウォータマークの入ったオブジェクトに対して大幅に劣ることとなる。当該技術者には、むやみに実験を行わずとも、特定のオブジェクトについて、スペクトルのどの部分を変調すべきかが分かるであろう。

【００１８】

キーベクトルV_Vから、オリジナルオブジェクト$I_V(i,j)$の選択部分に挿入するために適用可能なウォータマークベクトルW_Vが得られる（ブロック110）。後述するように、ウォータマークベクトルW_Vは、ウォータマークの挿入のために選択されたオリジナルオブジェクト$I_V(i,j)$の特定部分によって決まる。ウォータマークベクトルV_Vとオリジナルオブジェクト$I_V(i,j)$の選択部分を組み合わせることによって、ウォータマークをオリジナルオブジェクト$I_V(i,j)$に組み込んだ後、ウォータマークの入ったオブジェクト$I_V'(i,j)$が得られる（ブロック112）。

【００１９】

本発明の好ましい実施態様をより明確に例示するため、以下ではビジュアルイメージにウォータマーキングを施す例について述べることにする。もちろん当該技術者であれば、本開示に基づいて、例えばオーディオデジタルオブジェクト、触覚デジタルオブジェクト等の上述のような他のタイプの物理的オブジェクトにも同様にウォータマーキングを施すことが可能であることが理解される。

【００２０】

例

このプロセスについては、一般に、下記の解説の通りであり、図３に例示される。

【００２１】

（１）m行及びn列のピクセルを備えたデジタルオブジェクトイメージ、ベクトル$I_V(i,j)$が得られる。MD5関数のような標準的メッセージアルゴリズムを利用して、$I_V(i,j)$におけるデータビットのメッセージダイジェストを計算し、メッセージダイジェストM_Vが求められる。

【００２２】

（２）RSA法又は楕円曲線のような暗号化法を用いて、メッセージダイジェストにサインして、所有権者のシグネチャが生成され、これによって暗号化メッセージダイジェスト、ベクトルS_Vが得られる。

【００２３】

（３）S_Vが、ウォータマークを構成するためのシグネチャのビットであると仮定する。例えば、S_Vは512ビットを有することが可能である。ｎ項目のベクトルU_Vが構成されるが、ここでｎはピクセルの列の数に対応する。代替的にベクトルは、行数ｍに対応するｍ項目を備えることも可能である。その場合には、行に関係する下記のステップは、代わりに列にも適用されるし、その逆も行われることになる。この例においてU_Vを構成する場合、第２ビット～第65ビットに、暗号化メッセージダイジェストS_Vの対応するビット（例えば最初の64ビット）が０か１かによって決まる変調値が割り当てられる。暗号化メッセージダイジェスト、ベクトルS_Vにおけるビットの残りには、０値が割り当てられる。S_Vの最初のビットには、ピクセルのDC成分に対応するように０の値が割り当てられる。例えばU_Vの第２～第65ビットにおけるあるビットには、S_Vにおける対応するビットが０の場合、－１の値が割り当てられ、S_Vにおける対応するビットが１の場合、U_Vのビットには１が割り当てられる。もちろんその値が一貫しており、結果生じるウォータマークによって、オブジェクトに過度の歪みが生じない限り、その変調は他のオプション値を備えることが可能であることが理解される。例えばU_Vにおけるあるビットが、－１の値を備える代わりに、２の値を割り当てられることが可能であり、U_Vにおける１のビットに、－１の値を割り当てることも可能である。さらにU_Vの最初のビットは、64を超えるか又は64未満のビットを備えることも可能である。しかしU_Vが大きくなると、ウォータマークを実施するのにより大きな計算力が必要になり、U_Vがより小さくなると、アタッカーによる破壊の恐れが増すことになる。U_Vの最初のビットは、ビジュアルイメージオブジェクトの概念的により重要な周波数である低周波数に対応する。またこれは、オーディオデジタル作品にも当てはまる。しかし知覚上重要なビットが高周波数である他の作品の場合、U_Vの高周波数ビットが変調されることになる

と考えられる。さらにU_Vの最初のビットは、S_Vの最初のビットに基づく必要はなく、一貫性がある限り、随意的に他の何らかのビットに基づくことが可能である。例えばU_Vの最初のビットは、S_Vの最後のビット、中間のビット又は代替ビット等に基づくことが可能である。０の値を備えたS_Vの最初のビット（DC成分に対応する）によって、ウォータマークは輝度又はコントラストの変化に対する耐性を備えるようになる。

【００２４】

（４）キーベクトルV_Vを得るため、U_Vの逆フーリエ変換が実施される。もちろん例えば逆離散コサイン変換（DCT）のような他の他のタイプの変換を利用して、周波数領域から、例えば時間領域（例えばオーディオ及び他の時間変化信号）又は空間領域（例えばイメージ、ビデオ又は他の空間的変化信号）に、U_Vを変換することが可能である。当該技術者には、こうした変換を選択して、適用し、本開示に基づいてキーベクトルV_Vを求め、ウォータマークを導き出す方法が分かるであろう。

【００２５】

（５）オリジナルオブジェクト$I_V(i,j)$の一部、例えばｂの連続行が選択され、この部分を平均化して、直交化計算のため、イメージピクセルに関連した基準ベクトルA_Vが作成される。この例の場合、基準ベクトルA_Vは、平均化データによって計算される平均ベクトルである。オブジェクトに応じて、オブジェクト全体を選択したい場合もあれば、概念的に重要な細部を備えたその一部を選択したい場合もある。例えばｂは、イメージの中央セクションにおける16とすることが可能であるが、これは中央セクションの16行を平均化して、ベクトルA_Vを形成することを表している。次にキーベクトルV_VがベクトルA_Vに依存することになる、すなわちオブジェクトのｂ行における要素の列位置に依存することになる危険を軽減するために、基準ベクトルA_Vに対してキーベクトルV_Vを直交化させ、これによってウォータマークベクトルW_Vを得ることが望ましい。直交化は、下記の式１によって表すことが可能である：

【００２６】

【数１】

$$W = V - (\hat{V} \cdot \hat{A})A \qquad \text{式1}$$

$$\text{ここで} \quad \hat{V} = \frac{V}{\sqrt{V \cdot V}}$$

$$\text{及び} \quad \hat{A} = \frac{A}{\sqrt{A \cdot A}}$$

【００２７】

ここで

【００２８】

【数２】

$\hat{A}$

【００２９】

はA_Vに沿った単位ベクトルである。ウォータマークベクトルW_Vは、オリジナルオブジェクト$I_V(i,j)$に組み込まれることになるデジタルウォータマークの周波数及び大きさのデータを表している。

【００３０】

（６）ウォータマークベクトルW_Vは、基準ベクトルA_Vが導き出された$I_V(i,j)$の一部に挿入することによって、オリジナルオブジェクト、ベクトル$I_V(i,j)$に組み込まれることが好ましい。ウォータマークベクトルW_Vを挿入する一般的な方法は、以前に基準ベクトルA_Vに対して選択されたｂ行のそれぞれにW_Vの小スケーリングを施されたバージョンを加えることによる。オブジェクトのウォータマークの入った要素$I_V'(i,j)$を取得するこの方法は、下記の式によって表すことが可能である：

$$I_V'(i,j) = I_V(i,j) + a_V(i,j)\, W_V(i,j) \qquad \text{式2}$$

式２において、ａは比例定数であり、好ましい場合ｉ又はｊの位置に応じて変化する可能性がある。

望ましい実施態様の場合、

$$I_V(i,j) = c \times \cos(2\pi i / b) \qquad \text{式3}$$

一般にｃは、ウォータマーク信号がおよそ－40dB PSNR（ピークＳ／Ｎ比）であ

るように選択される。ウォータマークの他の挿入方法を利用することも可能である。例えば他のスケーリングファクタによって決まる複数スケーリングファクタａを利用することが可能である。同じキーベクトルV_Vを利用して、直交化ステップ及びウォータマーキングステップを繰り返すことによって、所望に応じて、デジタルオブジェクトの他の位置に追加ウォータマークを加えることが可能である。ウォータマークファクタを利用してウォータマークを組み込む代替的な方法については、本開示に基づき、当該技術者には明らかである（例えば参考までに本明細書において援用されている上述のCoxらによる文献を参照されたい）。図３に示す例の場合、オリジナルデジタルオブジェクトのｂ行が、ウォータマークの入ったピクセルのｂ行に置換される。したがってウォータマークの入ったオブジェクト$I_V'(i,j)$（オリジナルオブジェクトと同じ行数ｍ及び同じ列数ｎを備えている）には、ｂ行のウォータマークの入った要素が含まれるが、残りの（ｍ－ｂ）行の要素は、オリジナルデジタルオブジェクトにおける同じ行から不変のままである。結果生じるウォータマークは一次元ウォータマークであり、これは式２～３又は他の同様の式におけるｉ又はｊの変化に全ての列を必要とする。この一次元ウォータマークは、W_Vが行及び列の関数として変化する二次元ウォータマークよりも数学的に単純である。しかし所望の場合には、ウォータマーク行列W_{VM}が一方向ハッシュ関数及び暗号化プロセスから導き出される要素を備えるように、二次元ウォータマークを生成することも可能である。例えばW_{VM}は、さまざまな比例定数を備えたV_VをW_{VM}のそれぞれの列及び行の要素に組み込むことによって、V_Vから導き出すことが可能である。この以上の説明は、単なる一例であり、当該技術者には、本開示から二次元ウォータマークを導き出す方法が分かるであろう。

【００３１】

ウォータマークの入ったオブジェクト$I_V'(i,j)$から導き出された（例えばコピーされた）疑いのある被疑イメージ、ベクトル$I_V''(i,j)$が与えられると、図４に例示される以下の方法によって、その被疑イメージを評価することが可能である。この方法は、ウォータマークベクトルV_V及び平均行ベクトルA_Vを必要とする。この方法の場合、ウォータマークに関する被疑イメージにおけるｂの

連続行からなる各ブロックが、順次評価される。例えば最初のｂの連続行を評価し、次に第２の行から始まり、（１＋ｂ）番目の行に至るｂの連続行を評価し、さらに第３の行から（２＋ｎ）番目の行に至る連続行を評価し、以下同様に順次評価することが可能である。

【００３２】

（Ａ）評価すべき各ブロック毎に、ｂ行を平均化して基準ベクトルA_V''が求められる。

【００３３】

（Ｂ）A_Vに対してベクトルA_V''を直交化して、被疑ウォータマークベクトルX_Vが求められる。A_V''を直交化する数学的処理は、式１においてキーベクトルV_Vを直交化する数学的処理と同様である。

【００３４】

（Ｃ）W_Vに対するX_Vの相対的近似が、例えばW_VとX_Vの間の相関を計算することによって計算される。X_VとW_Vの間の相関を計算するための式は次の通りである：

【００３５】

【数３】

$$\text{相関関係} = \frac{W \cdot X}{\sqrt{(W \cdot W)(X \cdot X)}} \qquad \text{式４}$$

【００３６】

（Ｄ）ステップ（Ｃ）を繰り返して、ｂの連続行からなる全ブロックについて、W_Vに対するX_Vの相対的近似が計算される。次にｂ行からなる全ブロックにおける相対的近似の最大値が求められる。この相対的近似が所定のしきい値を超えると、被疑イメージはウォータマークを含んでいるものとみなされる。

【００３７】

（Ｅ）被疑イメージ、ベクトル$I_V''(i,j)$にクロッピング又はスケーリングが施される場合、基準ベクトルA_V''に沿った個々の照合位置を探索して、水平探索を実施することにより、最良の相対的近似を得ること、すなわち被疑オブジェクトに対するウォータマークの最大の相関に到達することが可能である。さら

に軸に関するデジタルオブジェクトの反射について、探索を実施することも可能である。

【００３８】

（Ｆ）V_Vと同じスペクトル特性を備えた、いくつかのランダムウォータマークベクトル候補（例えば100個のウォータマーク）が合成される。W_Vの相関が最大になった位置、スケール及びクロップファクタにおいて、これらのベクトル候補のそれぞれと被疑デジタルオブジェクト$I_V''(i,j)$の相関が計算される。

【００３９】

（Ｇ）オリジナルウォータマークから得られた相関が、ランダムベクトルについて得られた相関に対して比較される。前者と後者の隔たりが大きい場合、被疑オブジェクト$I_V''(i,j)$には、おそらくウォータマークキーベクトルV_Vが含まれている。換言すれば、被疑オブジェクト$I_V''(i,j)$は、おそらくオリジナルオブジェクト$I_V(i,j)$のウォータマークを備えており、したがっておそらくオリジナルオブジェクトから導き出されたものである。

【００４０】

上記は、被疑オブジェクトがオリジナルオブジェクトから導き出されたものであるか否かの検出について論じたものである。例えばデジタルイメージのような、デジタルオブジェクト、ベクトル$J_V(i,j)$の所有権が係争中である場合、裁判官のような中立の第三者によってウォータマークの存在が確認されることによって、その所有権が立証可能である。デジタルオブジェクトの所有権を主張する者は、$J_V(i,j)$に対応するオリジナルイメージ$I_V(i,j)$及びそのオリジナルデジタルオブジェクトのハッシュのシグネチャS_Vと、解読のための公開キーを裁判官に提示することになる。さらに所有権主張者は、ウォータマークを見つけることができるデジタルオブジェクト$J_V(i,j)$における位置と、オリジナルオブジェクト、ベクトル$I_V(i,j)$に対する$J_V(i,j)$のスケーリング及びクロッピングファクタを宣言することになる。裁判官は、下記のプロセスを利用して、検証することができる。

【００４１】

（Ａ）$I_V(i,j)$におけるビットのメッセージダイジェストを計算する。請求

者によって提示された公開キーによってS_Vを解読する。請求者が$J_V(i,j)$の所有権者であれば、計算されたメッセージダイジェスト及び解読されたS_Vに関するビットストリングは同じはずである。異なる場合には、請求者の所有権の請求を却下する。

【００４２】

（Ｂ）シグネチャS_VからウォータマークベクトルV_Vを作成する。オブジェクト$J_V(i,j)$の指定の位置において、クロッピング及びスケーリングに対する補正の後、ウォータマークベクトルV_Vの相関を計算する。オリジナルオブジェクト$I_V(i,j)$を利用して、対応する基準ベクトルA_Vを計算する。

【００４３】

（Ｃ）V_Vと同じスペクトル特性を備えたランダムウォータマーク候補を合成する。これらのベクトル候補のそれぞれとオブジェクト$J_V(i,j)$の相関を計算し、被疑デジタルオブジェクトにおけるウォータマークの存在を検出するための前述の方法のように、V_Vに関して得られた相関を、ランダムベクトル候補に関して得られた相関に対して比較する。２つの相関タイプの隔たりが大きければ、おそらくオブジェクト、ベクトル$J_V(i,j)$に、ウォータマークベクトルV_Vが含まれている、すなわち請求者によって提示されたオブジェクト$I_V(i,j)$のウォータマークが含まれている。

【００４４】

この例の場合、デジタルイメージが評価された。この例証となる例において利用されたオリジナルイメージオブジェクトが、図５の画像に示されている。オリジナルイメージオブジェクトは、256（m行）×384（ｎ列）のピクセルを備えている。図６には、ウォータマークの入ったイメージが示されている。ウォータマークの強度は、－45dB PSNRある。図５と図６を比較すると、人間の目に識別可能な知覚上の差が存在しないことが分かる。例えば目のような人間の感覚器官によって識別可能なものは、当該技術において既知のところであるか、あるいはむやみに実験を行わなくても判定することが可能である。図７には、上述の相関法を利用して、図６のウォータマークの入ったイメージに対する照合アルゴリズムによって得られる相関拡散が示されている。図７の場合、横座標は、イメージに

埋め込まれた真のウォータマークと同じスペクトル特性を備えた、種々の疑似のウォータマークが示されている。疑似のウォータマークは、照合アルゴリズムによって合成されたものである。図の中央のスパイク「sp」は、真のウォータマークを備えたイメージに適用された場合の相関に対応しており、一方グラフの残りの部分には、ランダムに生成されたウォータマークに適用された場合の相関、及び同じスペクトル幅の真のウォータマークが示されている。

【００４５】

クロッピング及び圧縮による歪みに対する耐性におけるウォータマークの堅牢さを評価するため、図５のデジタルオブジェクトにクロッピングを施すと、176×274ピクセルになり、JPEG圧縮を施すと、かなりの損失を生じて、28.6の圧縮比が得られた（JPEGは標準的な損失のある圧縮法であり、Bhaskaran and Konstantinides, Image and Video compression standards, Kluwer Publishersを参照されたい）。クロッピングされて圧縮を施されたイメージを圧縮解除すると、図８のイメージが得られた。図９は、図８のイメージに対する相関拡散が示されている。拡散の中央には、ウォータマークの存在を示す、したがって図９の画像が図５のイメージから導き出されたものであることを識別する、背の高いスパイク「spc」が明確に認められる。同様に、図５のイメージの縮小したバージョンを作成して、縮小したイメージの相関拡散（不図示）を計算することによって、縮小後に、ウォータマークが検証可能であることが示される。従って、ウォータマークがスケーリングに耐えることが明らかになる。さらに図10には、図６のウォータマークの入ったイメージにおける各８ビットピクセルの５つの最下位ビットをゼロに設定して、切り捨てた後の図５のイメージの画像が示されている。図11には、図10のイメージについて、検出手順を通じて処理を施すことによって得られた相関拡散が示されている。やはり相関拡散に明確なスパイク「spt」が認められる。したがって切り捨てに関するこの評価によって、ウォータマークが切り捨てに耐えることが明らかになる。

【００４６】

本発明にしたがう、デジタルオブジェクトにウォータマークを施し、ウォータマークの存在について被疑デジタルオブジェクトの評価を行う技法が、上述の式

に基づいて、データ操作及び計算を行うことが可能なデジタル電子装置によって実施可能である。このような適用可能なデジタル電子装置には、マイクロプロセッサ及び、例えばパーソナルコンピュータ、ミニコンピュータ、汎用コンピュータのようなコンピュータが含まれる。さらにデータ操作及び計算のためのアルゴリズムは、コンパクトディスク、フロッピディスク、ハードディスク、磁気テープ等のようなデジタル記憶装置に記憶することが可能であり、その上で、これをマイクロプロセッサ又はコンピュータにロードするか、あるいは読み取って、ウォータマーキング及び評価プロセスを実施することが可能である。このようなデジタル記憶装置は、一般にマイクロプロセッサ又はコンピュータによって読み取り可能な、適合するデジタル記憶媒体を備えた製品である。またコンピュータ間においてデジタルオブジェクトを転送し、ウォータマークを入れ及びウォータマークの評価を行うことができるように、各種コンピュータをネットワーク化することも考えられる。また言うまでもないが、異なるコンピュータ及びプロセッサによって、上述のウォータマーキングプロセスにおけるそれぞれのステップを個別に実施し、その結果を組み合わせて、ウォータマーキング又はウォータマークの存在に関する評価、並びにその両方の全機能を実現することが可能である。

【００４７】

本発明の望ましい実施態様について詳細に解説し、例示してきたが、もちろん当該技術者であれば、本発明の範囲内で修正を加えることが可能であることが理解される。

【図面の簡単な説明】

【図１】

本発明のウォータマーキング技法の実施態様を示すブロック図である。

【図２】

図１のウォータマーキング技法の実施態様をさらに詳細に示すブロック図である。

【図３】

本発明にしたがってデジタルオブジェクトから得られるウォータマーク付きオブジェクトの実施態様に関する流れ図である。

【図４】

本発明の実施態様の技法にしたがって、被疑オブジェクトを評価し、それがウォータマーク付きオブジェクトから導き出されたものか否かの判定を行う方法を示す図である。

【図５】

デジタルイメージから印刷された画像を示す図である。

【図６】

図５のデジタルイメージに組み込まれたウォータマークを備えるデジタルイメージから印刷された画像を示す図である。

【図７】

図６の相関拡散を示す図である。

【図８】

圧縮及びクロッピングによる歪みに対する耐性を示す、図５のクロッピング及びJPEG圧縮を施されたウォータマーク付きイメージを示す図である。

【図９】

オブジェクトにクロッピング及び圧縮が施されている場合でも、オブジェクトにおけるウォータマークの存在に関する評価の感度を示す、図８の相関拡散を示す図である。

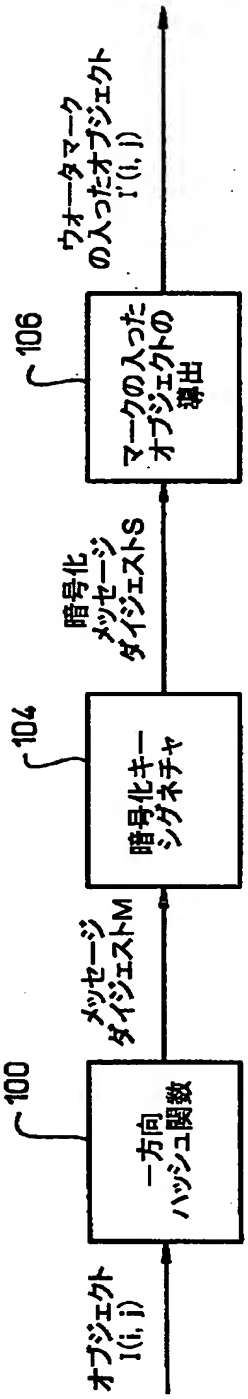
【図１０】

切り捨てによる歪みに対する耐性を示す、図５の切り捨てられたウォータマーク付きイメージを示す図である。

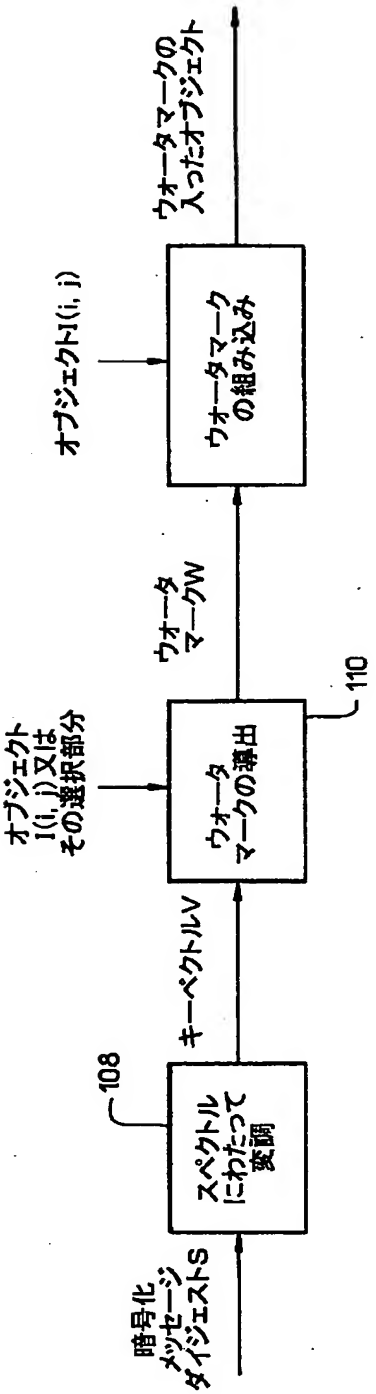
【図１１】

オブジェクトが切り捨てられている場合でも、オブジェクトにおけるウォータマークの存在に関する評価の感度を示す、図１０の相関拡散を示す図である。

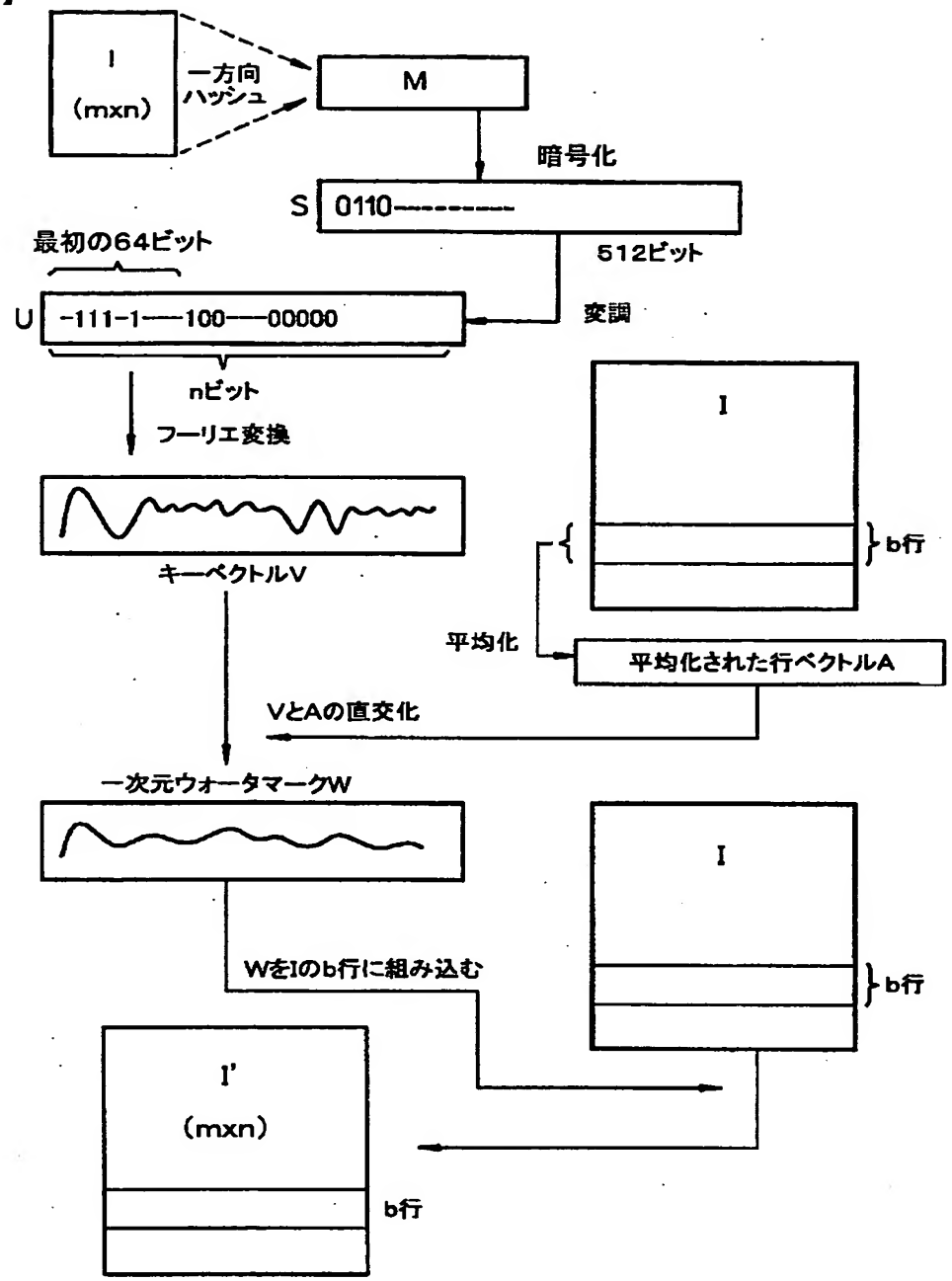
【図１】


オブジェクト
I(i, j)
100
一方向
ハッシュ関数
メッセージ
ダイジェストM
104
暗号化キー
シグネチャ
暗号化
メッセージ
ダイジェストS
106
マークの入った
オブジェクトの
導出
ウォータマーク
の入ったオブジェクト
I'(i, j)

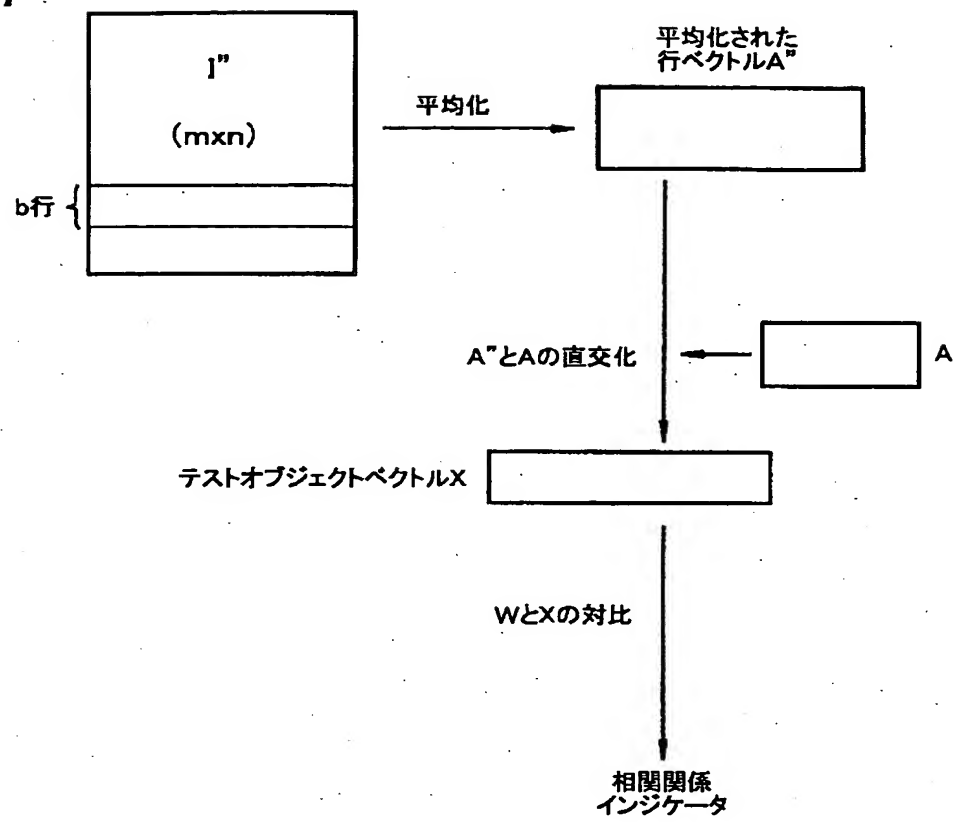
【図２】


暗号化
メッセージ
ダイジェストS
108
スペクトル
にわたって
変調
キーベクトルV
オブジェクト
I(i, j)又は
その選択部分
110
ウォータ
マークの導出
ウォータ
マークW
オブジェクトI(i, j)
ウォータマーク
の組み込み
ウォータマークの
入ったオブジェクト

【図３】


I
(mxn)
一方向
ハッシュ
M
暗号化
S
0110----------
512ビット
最初の64ビット
U
-111-1---100---00000
変調
nビット
フーリエ変換
キーベクトルV
I
b行
平均化
平均化された行ベクトルA
VとAの直交化
一次元ウォータマークW
I
Wを1のb行に組み込む
b行
I'
(mxn)
b行

【図４】


I"
(mxn)
b行
平均化
平均化された
行ベクトルA"
A"とAの直交化
A
テストオブジェクトベクトルX
WとXの対比
相関関係
インジケータ

【図５】

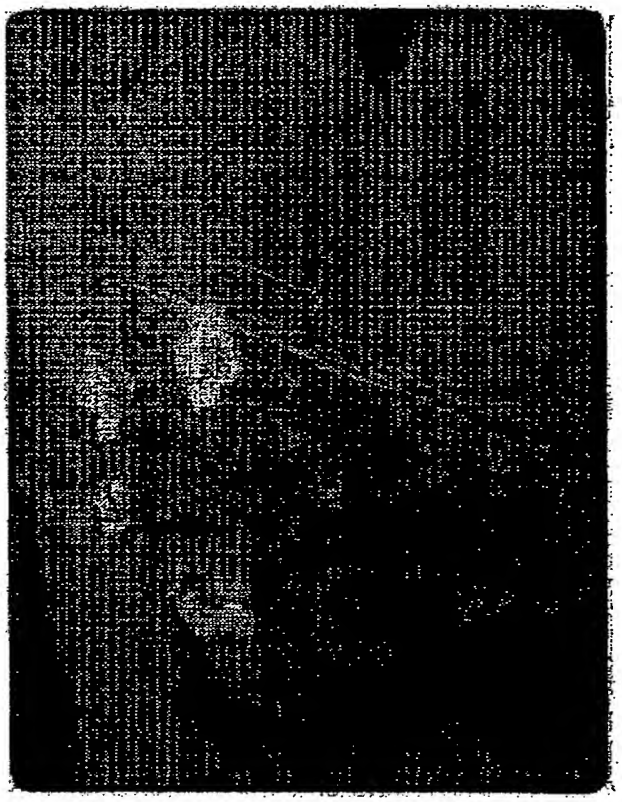


Fig. 5

【図６】

Fig. 6

【図７】

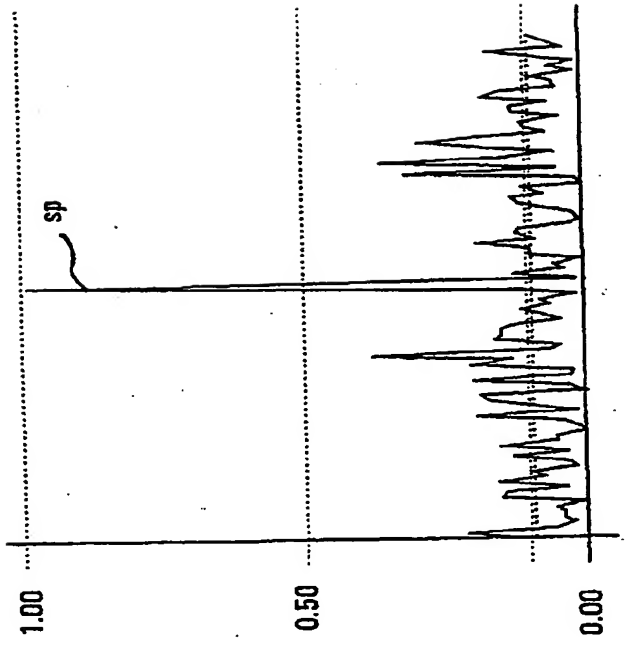


Fig. 7

【図８】

Fig. 8

【図９】

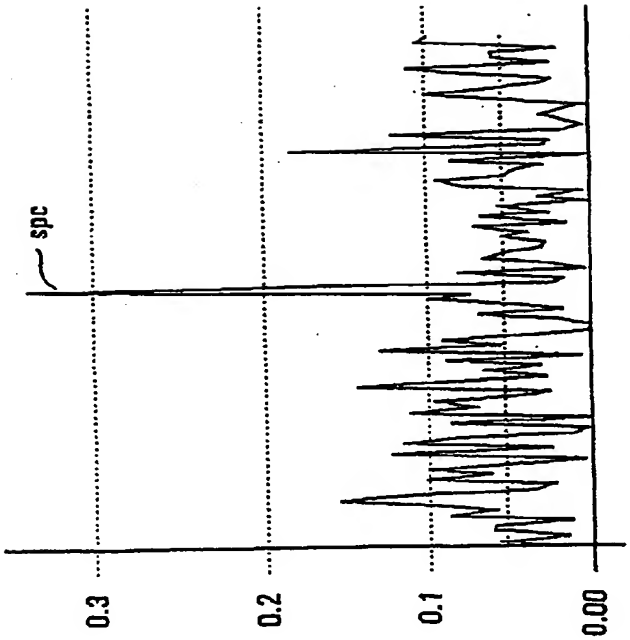


Fig. 9

【図１０】

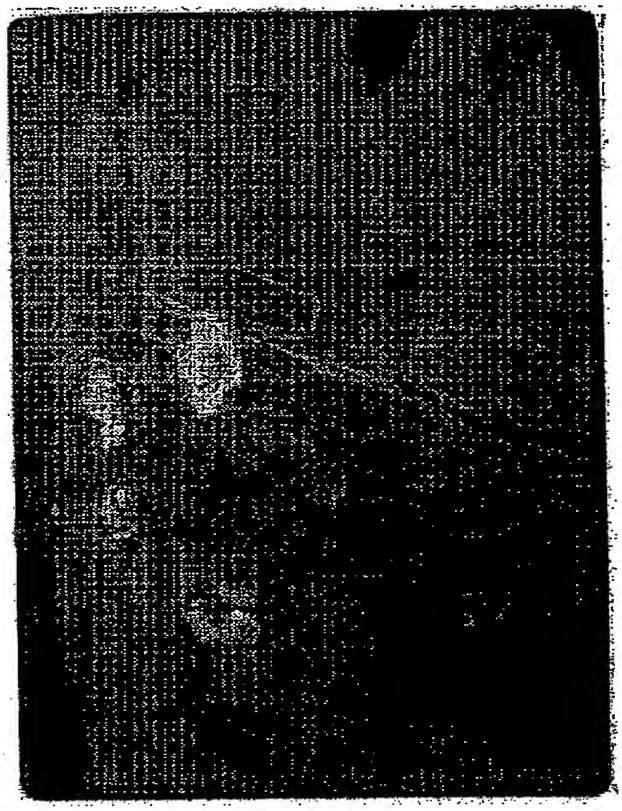


Fig. 10

【図１１】

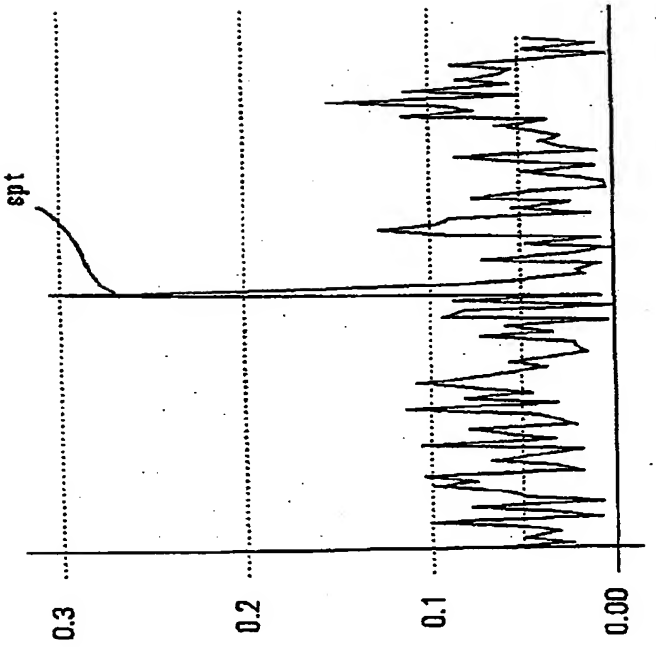


Fig. 11

【手続補正書】特許協力条約第３４条補正の翻訳文提出書

【提出日】平成１２年３月２７日（２０００．３．２７）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項１】デジタルウォータマークを利用して、デジタルオブジェクトを識別するための方法であって、

（ａ）前記デジタルオブジェクトのソースデータからハッシュ関数により導き出されたメッセージを暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るステップと、

（ｂ）前記暗号化メッセージダイジェスト（Ｓ）からウォータマークを導き出して、前記ソースデータに組み込み、それによって該ウォータマークが変更に対して耐性を備え、被疑データから生じるデータにハッシュ関数を実施することなく、該ウォータマークが依然として被疑データから見分けられるステップと

を含む方法。

【請求項２】前記メッセージが、前記デジタルオブジェクトの前記ソースデータにハッシュ関数を実施して、前記デジタルオブジェクトのメッセージダイジェスト（Ｍ）を得ることによって得られることと、前記メッセージダイジェスト（Ｍ）が、前記暗号化メッセージダイジェスト（Ｓ）を得るため、シグネチャ暗号化キーによって暗号化されるメッセージである、請求項１に記載の方法。

【請求項３】前記ウォータマークが物理領域のウォータマークであり、さらに前記ソースデータの少なくとも一部に前記物理領域のウォータマークを組み込むステップが含まれる、請求項１に記載の方法。

【請求項４】さらに前記ウォータマークを導き出す際、前記暗号化メッセージダイジェスト（Ｓ）から導き出された周波数領域ベクトル（Ｕ）を前記物理領域に変換するステップを含む、請求項３に記載の方法。

【請求項５】さらに前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調して、前記周波数領域ベクトル（Ｕ）の少なくとも一部を得ることによって、前記周波数領域ベクトル（Ｕ）を導き出すステップを含む、請求項４に記載の方法。

【請求項６】前記周波数領域ベクトル（Ｕ）の一部が低周波数に対応し、前記周波数領域ベクトル（Ｕ）の別の一部が高周波数に対応し、低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調することによって導き出される、請求項５に記載の方法。

【請求項７】低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、前記ウォータマークの振幅に対して、高周波数に対応する前記周波数領域ベクトル（Ｕ）の一部よりも重要な影響を及ぼすように変調されている、請求項６に記載の方法。

【請求項８】低周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部の「０」ビットに対応する要素に負の値を有し、かつ前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部の「１」ビットに対応する要素に正の値を有し、高周波数に対応する前記周波数領域ベクトル（Ｕ）の一部が、ゼロ値の要素を備える、請求項７に記載の方法。

【請求項９】前記ソースデータがデータユニットの行及び列から構成され、前記ウォータマークが、前記データユニットの前記行の数（ｍ）又は前記列の数（ｎ）に対応する次元を備えるウォータマークベクトル（Ｗ）によって表され、さらに

（ｃ）前記メッセージダイジェスト（Ｍ）から生じるデータを解読することなく、被疑ソースデータ内のウォータマークの存在を検出するステップを含む、請求項１に記載の方法。

【請求項１０】データユニットが、イメージオブジェクトの離散的セクションに関するデータを含む、請求項９に記載の方法。

【請求項１１】データユニットが、オーディオオブジェクトの離散的セクシ

ョンに関するデータを含む、請求項９に記載の方法。

【請求項１２】前記ソースデータに組み込まれた前記ウォータマークが、前記ウォータマークを付加されるデータに対して直交する、請求項９に記載の方法。

【請求項１３】さらに前記ソースデータの少なくとも一部を選択することによって、前記ソースデータからウォータマークベクトル（Ｗ）と同じ次元を備えたソースデータベクトル（Ａ）を導き出すステップを含み、さらに前記ウォータマークベクトル（Ｗ）がソースデータベクトル（Ａ）と直交するように、前記暗号化メッセージダイジェスト（Ｓ）に基づいて前記ウォータマークベクトル（Ｗ）を導き出すステップを含み、さらに前記ウォータマークベクトル（Ｗ）と、ソースデータベクトル（Ａ）が導き出される前記ソースデータの前記選択部分におけるデータを組み合わせて、ウォータマークの入ったデータを形成するステップを含む、請求項９に記載の方法。

【請求項１４】さらに前記ウォータマークの組み込み前を前記ウォータマークの組み込み後に対して、前記ソースデータの少なくとも一部を比較するステップを含む、請求項９に記載の方法。

【請求項１５】さらに前記ソースデータの少なくとも一部分を選択することによって、前記ウォータマークベクトル（Ｗ）と同じ次元を備えたソースデータベクトル（Ａ）をソースデータから導き出すステップを含み、さらに前記ウォータマークベクトル（Ｗ）と前記ウォータマークを含んでいることが疑われるデータから導き出される目標ベクトル（Ｘ）との間の相関関係を見出すステップを含み、前記目標ベクトル（Ｘ）が、前記ウォータマークの組み込まれている前記ソースデータに対して直交する、請求項１４に記載の方法。

【請求項１６】デジタルウォータマークを利用してデータを識別するための請求項１記載の方法であって、

（ａ）ソースデータからのデータに一方向ハッシュ関数を実施して、メッセージダイジェスト（Ｍ）を得るステップと、

（ｂ）シグネチャ暗号化キーによって前記メッセージダイジェスト（Ｍ）を暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るステップと、

（ｃ）前記暗号化メッセージダイジェスト（Ｓ）の高周波数に対応する部分より多い低周波数に対応する部分を変調することによって、前記暗号化メッセージダイジェスト（Ｓ）から周波数領域ベクトル（Ｕ）を導き出すステップと、

（ｄ）前記周波数領域ベクトル（Ｕ）を物理領域キーベクトル（Ｖ）に変換するステップと、

（ｅ）前記ソースデータの一部を選択して、前記選択されたソースデータに直交する周波数領域ベクトル（Ｕ）からウォータマークベクトル（Ｗ）を導き出すステップと、

（ｆ）前記選択されたソースデータと前記ウォータマークベクトル（Ｗ）を物理領域において組み合わせるステップと

（ｇ）前記メッセージダイジェストから生じるデータを解読することなく、かつ被疑ソースデータから生じるデータにハッシュ関数を実施することなく、被疑ソースデータ内のウォータマークの存在を検出するステップと

からなる方法。

【請求項１７】デジタルウォータマークを利用してデータを識別するためのシステムであって、

（ａ）シグネチャ暗号化キーによってソースデータからハッシュ関数によって導き出されたメッセージを暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るための手段と、

（ｂ）前記暗号化メッセージダイジェストからウォータマークを導き出して、前記ソース・データに組み込み、それによって該ウォータマークが変更に対して耐性を備え、被疑データから生じるデータにハッシュ関数を実施することなく、該ウォータマークが依然として被疑データから見分けるための手段と

を含むシステム。

【請求項１８】さらに前記ソースデータにハッシュ関数を施して、メッセージダイジェスト（Ｍ）を得るための手段を含み、前記暗号化するための手段が、シグネチャ暗号化キーによって前記メッセージダイジェスト（Ｍ）を暗号化して、前記暗号化メッセージダイジェスト（Ｓ）を得る、請求項１７に記載のシステム。

【請求項１９】前記ウォータマークが物理領域ウォータマークであり、前記導き出す手段が、前記物理領域ウォータマークを前記ソースデータの少なくとも一部に組み込む、請求項１７に記載のシステム。

【請求項２０】前記導き出す手段が、前記暗号化メッセージダイジェスト（Ｓ）から周波数領域ベクトル（Ｕ）を導き出し、前記ウォータマークを導き出す際、前記周波数領域ベクトル（Ｕ）を物理領域に変換し、さらに

（ｃ）前記メッセージダイジェスト（Ｍ）から生じるデータを解読することなく、被疑ソースデータ内のウォータマークの存在を検出するための手段を備える、請求項１９に記載のシステム。

【請求項２１】前記導き出す手段が、前記暗号化メッセージダイジェスト（Ｓ）の少なくとも一部を変調し、前記周波数領域ベクトル（Ｕ）の少なくとも一部を得ることによって、前記周波数領域ベクトル（Ｕ）を導き出す、請求項２０に記載のシステム。

【請求項２２】前記導き出す手段が、前記ソースデータをピクセル行及び列として管理し、前記周波数領域ベクトル（Ｕ）に基づいてウォータマークベクトル（Ｗ）を導き出し、前記ウォータマークベクトル（Ｗ）が、前記ピクセルの行の数（ｍ）又は前記列の数（ｎ）に対応する次元を備えている、請求項２１に記載のシステム。

【請求項２３】前記導き出す手段が、前記ソースデータの少なくとも一部を選択することによって、前記ソースデータから前記ウォータマークベクトル（Ｗ）と同じ次元を備えるソースデータベクトル（Ａ）を導き出し、前記ウォータマークベクトル（Ｗ）が、ソースデータベクトル（Ａ）に直交する、請求項２２に記載のシステム。

【請求項２４】さらに目標データセットを前記ソースデータと比較するための手段が含まれ、前記比較するための手段が、前記目標データから導き出された目標ベクトル（Ｘ）を前記ソースデータと比較し、前記目標ベクトル（Ｘ）が前記ソースデータベクトル（Ａ）に対して直交する、請求項２３に記載のシステム。

【請求項２５】コンピュータによる読み取りが可能なプログラムコード手段

を具体的に体現し、デジタルウォータマークを利用して、コンピュータにデジタルオブジェクトを識別させる、プログラム記憶媒体を備える製品であって、

（ａ）前記デジタルオブジェクトのソースデータからのデータに対して一方向ハッシュ関数を実施して、前記ソースデータのメッセージダイジェスト（Ｍ）を得るためのコード手段と、

（ｂ）シグネチャ暗号化キーによってメッセージダイジェスト（Ｍ）を暗号化して、暗号化メッセージダイジェスト（Ｓ）を得るためのコード手段と、

（ｃ）周波数領域としての前記暗号化メッセージダイジェスト（Ｓ）の一部を物理領域に変換することによって、前記暗号化メッセージダイジェスト（Ｓ）からウォータマークを導き出した後、前記ソースデータに組み込む一次元ウォータマークが得られるようにするためのコード手段と、

（ｄ）前記一次元ウォータマークを前記ソースデータに組み込むためのコード手段と、それによって該ウォータマークが変更に対して耐性を備え、被疑データから生じるデータに一方向ハッシュ関数を実施することなく、該ウォータマークが依然として被疑データから見分けられることと、

が含まれている製品。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００６

【補正方法】変更

【補正内容】

【０００６】

【発明が解決しようとする課題】

したがって本発明の目的は、クロッピングに耐え、可逆性であり、輝度又はコントラストの変化に耐える、また１つのウォータマークの入った作品におけるウォータマーキング技法が開示されても、他の関連するウォータマークの入った作品を危険にさらすことのない、ウォータマーキング技法を提供することにある。

Schneider M.らの「A Robust Content Based Digital Signature For Image Authenication,」Proceedings of the 1996 IEEE international conference in

Image Processing, vol. 3, 16-19 September, pages227-230, XP002090178 は、シグネチャをもとにして内容を表すための方法を開示し、この方法は、イメージを修正するタイプとは異なるタイプである。Delaigle, J.F.らの「Digital watermarking,」Proceedings of the SPIE, vol. 2659, 1 February 1996, pages 99-110, XP000604065 は、デジタル写真に目に見えないウォータマークを付けるプロセスを開示する。ウォータマークの検出には相関プロセスを必要とする。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】００１８

【補正方法】変更

【補正内容】

【００１８】

キーベクトルV_Vから、オリジナルオブジェクト$I_V(i,j)$の選択部分に挿入するために適用可能なウォータマークベクトルW_Vが得られる（ブロック110）。後述するように、ウォータマークベクトルW_Vは、ウォータマークの挿入のために選択されたオリジナルオブジェクト$I_V(i,j)$の特定部分によって決まる。ウォータマークベクトルW_Vとオリジナルオブジェクト$I_V(i,j)$の選択部分を組み合わせることによって、ウォータマークをオリジナルオブジェクト$I_V(i,j)$に組み込んだ後、ウォータマークの入ったオブジェクト$I_V'(i,j)$が得られる（ブロック112）。

【手続補正４】

【補正対象書類名】明細書

【補正対象項目名】００２６

【補正方法】変更

【補正内容】

【００２６】

【数１】

$$W = V - (V \cdot \hat{A})\hat{A} \qquad \text{式1}$$

ここで $\hat{V} = \dfrac{V}{\sqrt{V \cdot V}}$

及び $\hat{A} = \dfrac{A}{\sqrt{A \cdot A}}$

【手続補正５】

【補正対象書類名】明細書

【補正対象項目名】００３０

【補正方法】変更

【補正内容】

【００３０】

（６）ウォータマークベクトルW_Vは、基準ベクトルA_Vが導き出されたI_V（i,j）の一部に挿入することによって、オリジナルオブジェクト、ベクトルI_V（i,j）に組み込まれることが好ましい。ウォータマークベクトルW_Vを挿入する一般的な方法は、以前に基準ベクトルA_Vに対して選択されたｂ行のそれぞれにW_Vの小スケーリングを施されたバージョンを加えることによる。オブジェクトのウォータマークの入った要素I_V'（i,j）を取得するこの方法は、下記の式によって表すことが可能である：

$$I_V'(i,j) = I_V(i,j) + a_V(i,j)\, W_V(i,j) \qquad \text{式2}$$

式２において、a_Vは比例定数であり、好ましい場合ｉ又はｊの位置に応じて変化する可能性がある。

望ましい実施態様の場合、

$$a_V(i,j) = c \times \cos(2\pi i / b) \qquad \text{式3}$$

一般にｃは、ウォータマーク信号がおよそ－40dB　PSNR（ピークＳ／Ｎ比）であるように選択される。ウォータマークの他の挿入方法を利用することも可能である。例えば他のスケーリングファクタによって決まる複数スケーリングファクタa_Vを利用することが可能である。同じキーベクトルV_Vを利用して、直交化ステップ及びウォータマーキングステップを繰り返すことによって、所望に応じて、

デジタルオブジェクトの他の位置に追加ウォータマークを加えることが可能である。ウォータマークファクタを利用してウォータマークを組み込む代替的な方法については、本開示に基づき、当該技術者には明らかである（例えば参考までに本明細書において援用されている上述のCoxらによる文献を参照されたい）。図３に示す例の場合、オリジナルデジタルオブジェクトのｂ行が、ウォータマークの入ったピクセルのｂ行に置換される。したがってウォータマークの入ったオブジェクト$I_V'(i,j)$（オリジナルオブジェクトと同じ行数ｍ及び同じ列数ｎを備えている）には、ｂ行のウォータマークの入った要素が含まれるが、残りの（ｍ－ｂ）行の要素は、オリジナルデジタルオブジェクトにおける同じ行から不変のままである。結果生じるウォータマークは、式２～３又は他の同様の式におけるｉ又はｊの変化に全ての列を含むので、一次元ウォータマークである。この一次元ウォータマークは、W_Vが行及び列の関数として変化する二次元ウォータマークよりも数学的に単純である。しかし所望の場合には、ウォータマーク行列W_{Vm}が一方向ハッシュ関数及び暗号化プロセスから導き出される要素を備えるように、二次元ウォータマークを生成することも可能である。例えばW_{Vm}は、さまざまな比例定数を備えたV_VをW_{Vm}のそれぞれの列及び行の要素に組み込むことによって、V_Vから導き出すことが可能である。この以上の説明は、単なる一例であり、当該技術者には、本開示から二次元ウォータマークを導き出す方法が分かるであろう。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/US 98/20196

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE 1996 IEEE INTERNATIONAL CONFERENCE IN IMAGE PROCESSING, vol. 3, 16 - 19 September 1996, pages 227-230, XP002090178	1-3, 17-19
Y	see the whole document	4-7,20, 21
Y	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996, pages 99-110, XP000604065	4-7,20, 21
A	see the whole document	14-16,24

-/—

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 January 1999	28/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hubeau, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/20196

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 499 294 A (FRIEDMAN GARY L) 12 March 1996 see column 2, line 18 - column 3, line 25	1-3, 17-19

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/20196

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5499294 A	12-03-1996	NONE	

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

Fターム(参考) 5C059 KK43 RB02 RC35 SS30 UA02
5C075 EE03
5C076 AA14 BA06
5J104 AA14 NA12 NA22 PA07 PA14